

The second minimum of Barnes-Wall lattices

Gabriele Nebe*

Lehrstuhl für Algebra und Zahlentheorie, RWTH Aachen
University, Germany

ABSTRACT. We show that the second minimum of the Barnes-Wall lattices is at least $3/2$ of the minimum.

KEYWORDS: Barnes-Wall lattices, minima of lattices

1 Introduction

The Barnes-Wall lattices form an infinite series of lattices of dimension 2^m for $m \in \mathbb{N}$. They are constructed in [2] which explicitly elaborates their minimal vectors to show that the Barnes-Wall lattices are locally densest lattices. This fact also follows from an inspection of their automorphism group. For $m \neq 3$ this group is a subgroup of index 2 of the real Clifford group (see [9]), a fact that allows Bachoc in [1] to show that for $m \geq 3$ all non-empty layers of the Barnes-Wall lattices form spherical 6-designs.

The most prominent construction of the Barnes-Wall lattices is by applying Construction D to a chain of Reed-Muller codes (see for instance [5, Chapter 8, Section 8], [2], and also [7] for a basis-independent formulation). Berlekamp and Sloane [3] show that in the r -th order binary Reed-Muller code of length 2^m and minimum distance $d = 2^{m+r}$, the only codewords having weight between d and $2d$ are those with weights of the form $2d - 2^i$ for some i . Motivated by this observation, certain experiments, and the theta series of the Barnes-Wall lattice of dimension 64 and 128 in [11] Christoph Keller [8] conjectured that a similar property should also be true for the Barnes-Wall lattices.

The present note is a first step in this direction showing that the Barnes-Wall lattices of minimum d have no vectors of norm a with $d < a < 3d/2$.

*nebe@math.rwth-aachen.de

2 The two Barnes-Wall lattices of dimension 2^m

In [2] Barnes and Wall construct a series of lattices in dimension $N := 2^m$ for any $m \in \mathbb{N}$. Put $\mathcal{V}_m = \mathbb{F}_2^m$ to denote the m -dimensional vector space over the field with 2 elements and fix a basis $(v_1, \dots, v_m)$ of $\mathcal{V}_m$. Put

$$\mathcal{T}_r(m) := \{\mathcal{U} \leq \mathcal{V}_m \mid \mathcal{U} = \langle v_i \mid i \in I \rangle_{\mathbb{F}_2}, I \subseteq \{1, \dots, m\}, |I| = r\}$$

to denote the set of r -dimensional subspaces of $\mathcal{V}_m$ that have a basis that is a subset of $\{v_1, \dots, v_m\}$.

We now let $\mathcal{V}_m$ index the elements of an orthonormal basis

$$(e_v \mid v \in \mathcal{V}_m)$$

of the euclidean space $(\mathbb{R}^N, (\cdot, \cdot))$. Let

$$\Gamma_m := \langle e_v \mid v \in \mathcal{V}_m \rangle_{\mathbb{Z}}$$

denote the standard lattice spanned by this orthonormal basis. For any subset $\mathcal{U}$ of $\mathcal{V}_m$ we put

$$x_{\mathcal{U}} := \sum_{v \in \mathcal{U}} e_v \in \Gamma_m.$$

Then [2] defines the following sublattices of Γ_m :

Definition 2.1. Let $\lambda := (\lambda_0, \dots, \lambda_m) \in \mathbb{Z}^{m+1}$ such that $\lambda_0 = 0, \lambda_r - 1 \leq \lambda_{r-1} \leq \lambda_r$ for all $1 \leq r \leq m$. Then

$$\Lambda(\lambda) := \langle 2^{\lambda_{m-r}} x_{\mathcal{U}} \mid 0 \leq r \leq m, \mathcal{U} \text{ affine subspace of } \mathcal{V}_m, \dim(\mathcal{U}) = r \rangle_{\mathbb{Z}}.$$

For λ as in Definition 2.1 put $\lambda' := (\lambda'_0, \dots, \lambda'_m)$ where $\lambda'_r = \lambda_m - \lambda_{m-r}$. Then [2, Theorem 3.1, Theorem 3.2] give the following properties of the lattices $\Lambda(\lambda)$.

Proposition 2.2. (a) $\Lambda(\lambda') = 2^{\lambda_m} \Lambda(\lambda)^{\#}$.

(b) A $\mathbb{Z}$ -basis of $\Lambda(\lambda)$ is given by

$$\bigcup_{r=0}^m \{2^{\lambda_{m-r}} x_{\mathcal{U}} \mid \mathcal{U} \in \mathcal{T}_r(m)\}.$$

(c) $\det(\Lambda(\lambda)) = 2^{2d}$ where $d = \sum_{r=0}^m \lambda_r \binom{m}{r}$.

(d) $\min(\Lambda(\lambda)) = 2^{\alpha}$ where $\alpha = \min\{m - r + 2\lambda_r \mid 0 \leq r \leq m\}$.

Barnes and Wall single out two particular lattices among the lattices $\Lambda(\lambda)$:

Theorem 2.3. ([2, Theorem 4.3]) Put $\lambda_r := \lfloor \frac{r}{2} \rfloor$ and $\mu_r := \lfloor \frac{r+1}{2} \rfloor$ ($0 \leq r \leq m$) and put

$$\Lambda_m := \Lambda(\lambda), \quad \Delta_m := \Lambda(\mu).$$

The index of Λ_m in the standard lattice Γ_m is 2^j where

$$j = \log_2([\Gamma_m : \Lambda_m]) = \sum_{r=0}^m \lfloor \frac{r}{2} \rfloor \binom{m}{r} = (m-1)2^{m-2}.$$

Moreover Λ_m and Δ_m are similar lattices with a similarity factor 2, so $\Lambda_m \supset \Delta_m \supset 2\Delta_m$ with $[\Lambda_m : \Delta_m] = [\Delta_m : 2\Delta_m] = 2^{m-1}$. For the minimum of the two lattices we get $\min(\Lambda_m) = 2^{m-1}$, $\min(\Delta_m) = 2^m$.

The lattices that are commonly known as “the” Barnes-Wall lattices are scaled versions of the lattices Λ_m from Theorem 2.3.

Remark 2.4. If $m \geq 3$ is odd then $\text{BW}_m := 2^{-(m-1)/4} \Lambda_m$ is an even unimodular lattice of minimum $\min(\text{BW}_m) = 2^{(m-1)/2}$.

If m is even then $\text{BW}_m := 2^{-(m-2)/4} \Lambda_m$ is an even 2-modular lattice of minimum $\min(\text{BW}_m) = 2^{m/2}$.

The automorphism group $G_m \cong 2_+^{1+2m}.\Omega_{2m}(2)$ of Λ_m (for $m = 3$ we put G_m to denote the stabiliser of Δ_m in $\text{Aut}(\Lambda_m)$) is a normal subgroup of index 2 in the real Clifford group $\langle G_m, h \rangle \leq \text{GL}_N(\mathbb{R})$ (see for instance [1], [9]). The element $\sqrt{2}h$ is rational and induces the similarity between Λ_m and $\Delta_m = \sqrt{2}h\Lambda_m$. The group G_m is studied in detail in [4].

Theorem 2.5. ([4, Théorème II.4]) G_m acts transitively on the set of minimal vectors of Λ_m .

3 The second minimum of the lattices Λ_m .

3.1 The minimal classes in Λ_m/Δ_m

The key observation for having a recursive proof of the second minimum of the Barnes-Wall lattices is given in the following lemma.

Lemma 3.1. Let $\ell \in \Lambda_m$ be a minimal vector, i.e. $(\ell, \ell) = 2^{m-1}$. Then for any $x \in \ell + \Delta_m$ either $(x, x) = (\ell, \ell) = 2^{m-1}$ or $(x, x) \geq 2^m$.

Proof. By Theorem 2.5 the group G_m acts transitively on the set of minimal classes of Λ_m/Δ_m so we make a suitable choice of the minimal vector ℓ .

First assume that m is odd. Then we choose the minimal vector $\ell = 2^{(m-1)/2}e_0 \in \Lambda_m$ and let $x = \ell + d \in \ell + \Delta_m$ with $(x, x) > 2^{m-1}$. Write $x = \sum_{v \in \mathcal{V}_m} a_v e_v$ with

coefficients $a_v \in \mathbb{Z}$ in the orthonormal basis and let 2^j be the maximal 2-power that divides all a_v . If $j \geq (m-1)/2$ then (x, x) is a multiple of 2^{m-1} and hence $(x, x) \geq 2^m$ by the assumption that $(x, x) > 2^{m-1}$. So assume that $j < (m-1)/2$ and put

$$y := 2^{-j}x = \sum_{v \in \mathcal{V}_m} b_v e_v$$

with $b_v = 2^{-j}a_v \in \mathbb{Z}$. Then $2^{-j}d = (b_0 - 2^{(m-1)/2-j})e_0 + \sum_{0 \neq v \in \mathcal{V}_m} b_v e_v$ and the set $S := \{v \in \mathcal{V}_m \mid b_v \text{ odd}\}$ is the set of indices of the odd coefficients in $2^{-j}d$. By [2, Lemma 3.3] the cardinality of S is $\geq 2^{m-2j}$ and hence $(x, x) = 2^{2j}(y, y) \geq 2^{2j}|S| \geq 2^m$. This shows the lemma if m is odd.

For even m , there are no minimal vectors of Λ_m that are scalar multiples of one of the e_v . However, as Λ_m and Δ_m are similar, we may use the same argument as before for the minimal classes of $\Delta_m/2\Lambda_m$. So we choose the minimal vector $\ell = 2^{m/2}e_0 \in \Delta_m$ and assume that $d \in 2\Lambda_m$ is such that $x = \ell + d \in \ell + 2\Lambda_m$ has norm $(x, x) > 2^m = \min(\Delta_m)$. Then the same argument as before shows that $(x, x) \geq 2^{m+1}$ which shows the lemma also for m even. $\square$

3.2 A recursive construction of Λ_m as a subdirect product

The Barnes-Wall lattices have an easy construction as a subdirect product, very similar to the doubling construction for the Reed-Muller codes. Fixing the basis $(v_1, \dots, v_{m+1})$ of $\mathcal{V}_{m+1}$ as before, there is a natural embedding

$$\iota : \mathcal{V}_m = \langle v_1, \dots, v_m \rangle \hookrightarrow \mathcal{V}_{m+1}.$$

Combining ι with the translation along v_{m+1} we obtain a bijection

$$\tau : \mathcal{V}_m \rightarrow v_{m+1} + \iota(\mathcal{V}_m), v \mapsto v_{m+1} + \iota(v)$$

so that $\mathcal{V}_{m+1} = \iota(\mathcal{V}_m) \dot{\cup} \tau(\mathcal{V}_m)$. By abuse of notation we also use ι and τ to denote the $\mathbb{Z}$ -linear maps

$$\iota : \Gamma_m \rightarrow \Gamma_{m+1}, e_v \mapsto e_{\iota(v)} \text{ for all } v \in \mathcal{V}_m$$

and

$$\tau : \Gamma_m \rightarrow \Gamma_{m+1}, e_v \mapsto e_{\tau(v)} \text{ for all } v \in \mathcal{V}_m.$$

Then ι and τ are isometric embeddings and Γ_{m+1} is the orthogonal sum of $\iota(\Gamma_m)$ and $\tau(\Gamma_m)$. In this notation we obtain

Theorem 3.2. $\Lambda_{m+1} = \{\iota(\ell) + \iota(d) + \tau(\ell) \mid \ell \in \Lambda_m, d \in \Delta_m\}.$

Proof. The right hand side, Λ , is a lattice, in fact we have

$$\Lambda = (\iota + \tau)(\Lambda_m) \oplus \iota(\Delta_m).$$

So the index of Λ in Γ_{m+1} is 2^j with

$$j = \log_2([\Gamma_{m+1} : \Lambda]) = \log_2([\Gamma_m : \Delta_m]) + \log_2([\Gamma_m : \Lambda_m]) = (m+1)2^{m-2} + (m-1)2^{m-2} = m2^{m-1} = \log_2([\Gamma_{m+1} : \Lambda_{m+1}]).$$

So it remains to show that the basis of Λ_{m+1} given in Proposition 2.2 (b) is contained in Λ . So let $\mathcal{U} \in \mathcal{T}_r(m+1)$.

If $v_{m+1} \in \mathcal{U}$ then $\mathcal{U}' := \mathcal{U} \cap \mathcal{V}_m \in \mathcal{T}_{r-1}(m)$ and

$$2^{\lfloor \frac{m+1-r}{2} \rfloor} x_{\mathcal{U}} = \iota(2^{\lfloor \frac{m-(r-1)}{2} \rfloor} x_{\mathcal{U}'}) + \tau(2^{\lfloor \frac{m-(r-1)}{2} \rfloor} x_{\mathcal{U}'}) \in (\iota + \tau)(\Lambda_m).$$

If $v_{m+1} \notin \mathcal{U}$ then $\mathcal{U} \in \mathcal{T}_r(m)$ and

$$2^{\lfloor \frac{m+1-r}{2} \rfloor} x_{\mathcal{U}} = \iota(2^{\lfloor \frac{m-r+1}{2} \rfloor} x_{\mathcal{U}'}) \in \iota(\Delta_m).$$

□

For related constructions see for instance [6] and [10].

3.3 The main result

Theorem 3.3. *Let $x \in \Lambda_m$ be such that $(x, x) > \min(\Lambda_m) = 2^{m-1}$. Then $(x, x) \geq 2^{m-1} + 2^{m-2}$.*

Proof. We proceed by induction on m . The cases $m = 2, \dots, 5$ follow immediately from Remark 2.4, as here BW_m is an even lattice of minimum ≤ 4 .

For the induction step assume that the theorem holds for m and let $x = \iota(\ell) + \iota(d) + \tau(\ell) \in \Lambda_{m+1}$ with

$$2^m < (x, x) = (\ell + d, \ell + d) + (\ell, \ell) < 2^m + 2^{m-1}.$$

Without loss of generality we assume that $(\ell, \ell) \leq (\ell + d, \ell + d)$.

Then there are three cases to consider:

If $\ell = 0$, then $d \in \Delta_m$ is not a minimal vector as $(x, x) = (d, d) > 2^m$. Hence by induction hypothesis (using the fact that Δ_m is similar to Λ_m) we have $(x, x) = (d, d) \geq 2^m + 2^{m-1}$.

If $\ell \in \Lambda_m$ is not a minimal vector then by assumption $(\ell, \ell) \geq 2^{m-1} + 2^{m-2}$ and hence $(x, x) \geq 2(\ell, \ell) \geq 2^m + 2^{m-1}$.

In the last case $\ell \in \Lambda_m$ is a minimal vector, i.e. $(\ell, \ell) = 2^{m-1}$. By assumption $(x, x) > 2^m$, therefore $\ell + d \in \ell + \Delta_m$ is not a minimal vector, so $(\ell + d, \ell + d) \geq 2^m$

by Lemma 3.1. Therefore $(x, x) \geq 2^m + 2^{m-1}$.

Combining these three cases shows the claim for $m + 1$ and finishes the induction step. $\square$

The proof above also gives an easy recursive formula for the number

$$s_m := \{\ell \in \Lambda_m \mid (\ell, \ell) = 2^{m-1}\}$$

of minimal vectors in Λ_m :

Remark 3.4. The kissing number s_m of Λ_m satisfies $s_1 = 4$ and for $m \geq 2$

$$s_m = (2^m + 2)s_{m-1}.$$

Proof. For $\ell \in \Lambda_m$ with $(\ell, \ell) = 2^{m-1}$ the minimal vectors in $\ell + \Delta_m$ form a frame $\{\pm\ell_1, \pm\ell_2, \dots, \pm\ell_{2^m}\}$ i.e. $(\ell_i, \ell_j) = 0$ for $i \neq j$. This follows from the fact that both, $\ell_i \pm \ell_j$ are in Δ_m and hence

$$(\ell_i \pm \ell_j, \ell_i \pm \ell_j) = 2^m \pm 2(\ell_i, \ell_j) \geq 2^m = \min(\Delta_m).$$

So there are $2^m s_{m-1}$ minimal vectors of the form $(\iota + \tau)(\ell) + \iota(d) \in \Lambda_m$, where $\ell, \ell + d \in \Lambda_{m-1}$ are both minimal vectors and $2s_{m-1}$ minimal vectors of the form $\iota(d)$ or $\tau(d)$ where $d \in \Delta_{m-1}$ is a minimal vector. $\square$

References

- [1] Christine Bachoc, Designs, groups and lattices. J. Théor. Nombres Bordx. **17** (2005) 25-44.
- [2] E. S. Barnes, G. E. Wall, Some extreme forms defined in terms of Abelian groups. J. Aust. Math. Soc. **1** (1959) 47-63.
- [3] E. R. Berlekamp, N. J. A. Sloane, Restrictions on weight distribution of Reed-Muller codes. Inf. Control **14** (1969) 442-456.
- [4] Michel Broué, Michel Enguehard, Une famille infinie de formes quadratiques entières; leurs groupes d'automorphismes. Ann. scient. Éc. Norm. Sup. **6** (1973) 17-52.
- [5] J. H. Conway, N. J. A. Sloane, Sphere packings, lattices and groups. Springer, 3. edition (1998).
- [6] Robert L. Griess, Midwest cousins of Barnes-Wall lattices. J. Number Theory **130** (2010) 680-695.

- [7] Sihuang Hu, Gabriele Nebe, Strongly perfect lattices sandwiched between Barnes-Wall lattices. *J. Lond. Math. Soc., II. Ser.* **101** (2020) 1068-1089.
- [8] Christoph A. Keller (2025) private communication
- [9] G. Nebe, E. M. Rains, N. J. A. Sloane, The invariants of the Clifford groups. *Des. Codes Cryptography* **24** (2001) 99-121.
- [10] G. Nebe, E. M. Rains, N. J. A. Sloane, A simple construction for the Barnes-Wall lattices. Blahut, Richard E. (ed.) et al., *Codes, graphs, and systems. A celebration of the life and career of G. David Forney, Jr. on the occasion of his sixtieth birthday.* Boston, MA: Kluwer Academic Publishers. Kluwer Int. Ser. Eng. Comput. Sci. 670, 333-342 (2002).
- [11] OEIS Foundation Inc. (2026), The On-Line Encyclopedia of Integer Sequences, Published electronically at <https://oeis.org>